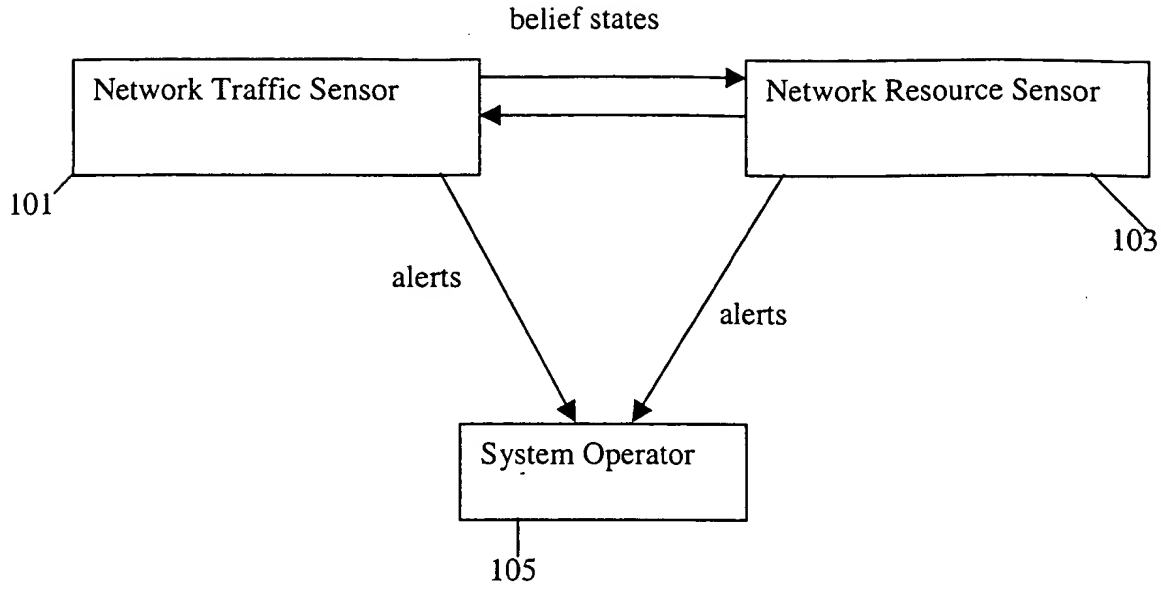
belief states
Network Traffic Sensor
Network Resource Sensor
101
103
alerts
alerts
System Operator
105
100

**FIGURE 1**

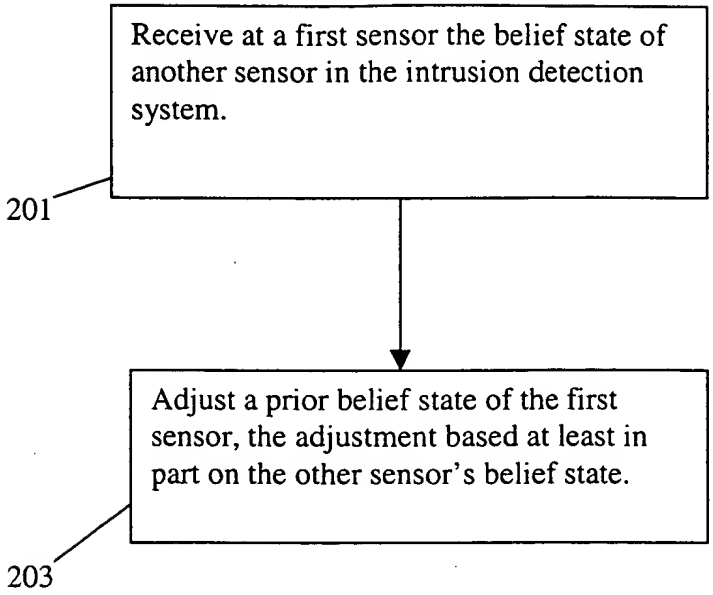


FIGURE 2

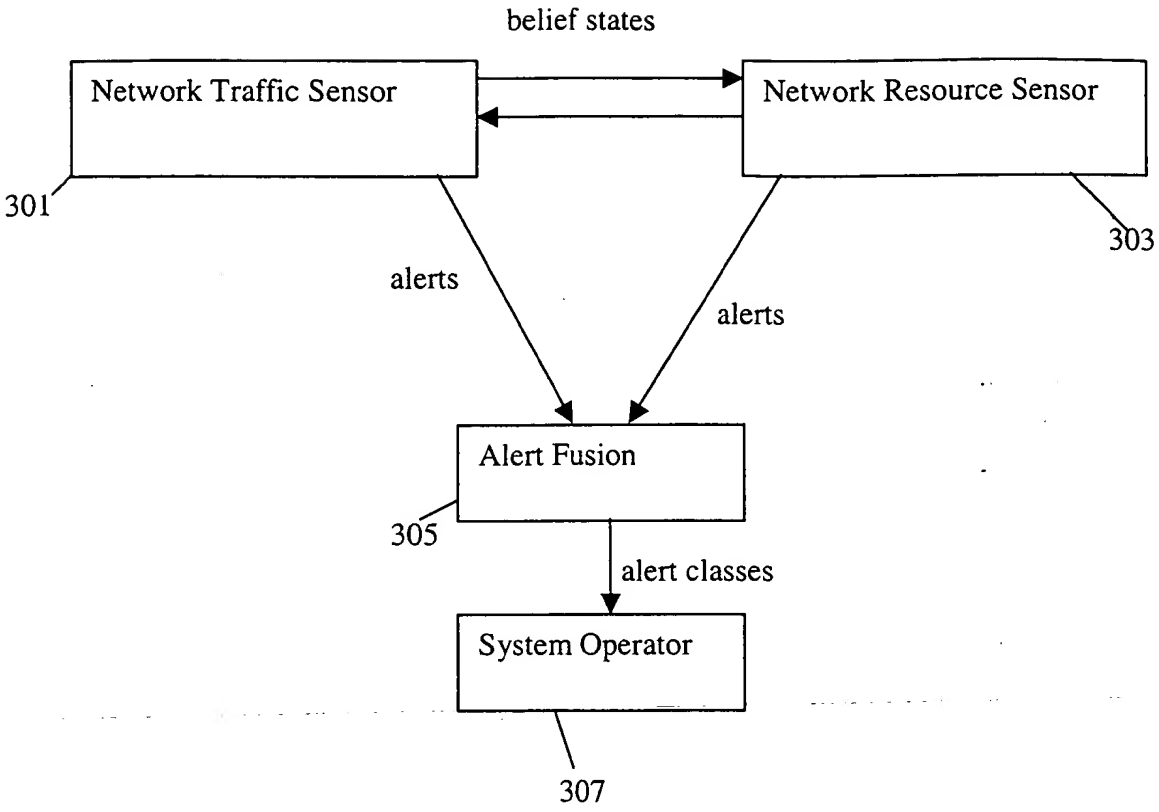
belief states
Network Traffic Sensor
Network Resource Sensor
301
303
alerts
alerts
Alert Fusion
305
alert classes
System Operator
307
300

**FIGURE 3**

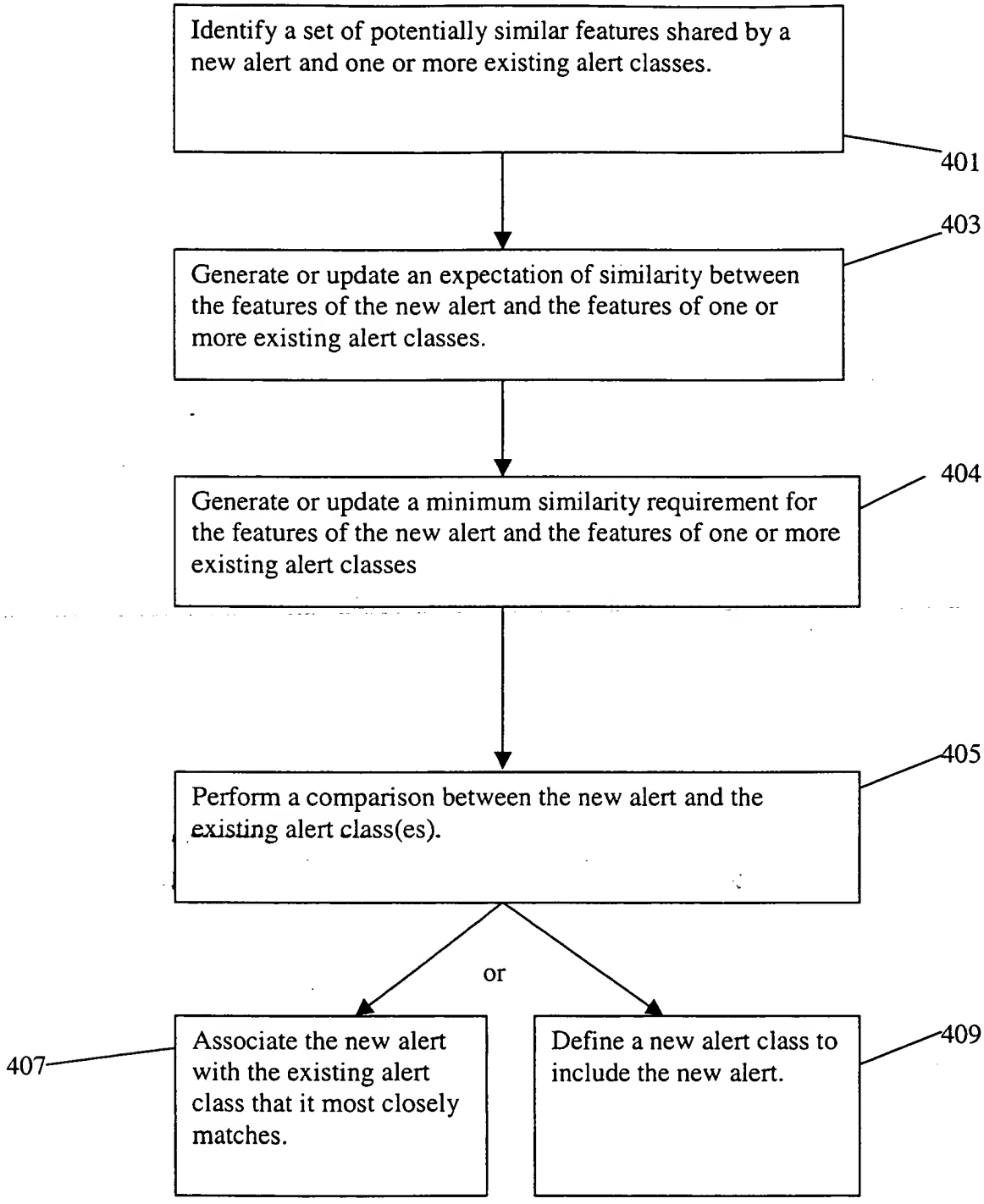
Identify a set of potentially similar features shared by a new alert and one or more existing alert classes.
401
403
Generate or update an expectation of similarity between the features of the new alert and the features of one or more existing alert classes.
404
Generate or update a minimum similarity requirement for the features of the new alert and the features of one or more existing alert classes
405
Perform a comparison between the new alert and the existing alert class(es).
or
407
Associate the new alert with the existing alert class that it most closely matches.
409
Define a new alert class to include the new alert.

FIGURE 4

| | INVALID | PRIVILEGE_VIOLATION | USER_SUBVERSION | DENIAL_OF_SERVICE | PROBE | ACCESS_VIOLATION | INTEGRITY VIOLATION | SYSTEM_ENV_CORRUPTION | USER_ENV_CORRUPTION | ASSET_DISTRESS | SUSPICIOUS_USAGE | CONNECTION_VIOLATION | BINARY_SUBVERSION | ACTION_LOGGED |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| INVALID | 1 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.6 |
| PRIVILEGE_VIOLATION | 0.3 | 1 | 0.6 | 0.3 | 0.6 | 0.6 | 0.6 | 0.6 | 0.4 | 0.3 | 0.4 | 0.1 | 0.5 | 0.6 |
| USER_SUBVERSION | 0.3 | 0.6 | 1 | 0.3 | 0.6 | 0.5 | 0.5 | 0.4 | 0.6 | 0.3 | 0.4 | 0.1 | 0.5 | 0.6 |
| DENIAL_OF_SERVICE | 0.3 | 0.3 | 0.3 | 1 | 0.6 | 0.3 | 0.3 | 0.4 | 0.3 | 0.5 | 0.4 | 0.1 | 0.5 | 0.6 |
| PROBE | 0.3 | 0.2 | 0.2 | 0.3 | 1 | 0.7 | 0.3 | 0.3 | 0.3 | 0.3 | 0.4 | 0.8 | 0.3 | 0.6 |
| ACCESS_VIOLATION | 0.3 | 0.6 | 0.3 | 0.5 | 0.6 | 1 | 0.6 | 0.6 | 0.3 | 0.3 | 0.4 | 0.1 | 0.5 | 0.6 |
| INTEGRITY VIOLATION | 0.3 | 0.5 | 0.3 | 0.5 | 0.6 | 0.8 | 1 | 0.6 | 0.5 | 0.3 | 0.4 | 0.1 | 0.5 | 0.6 |
| SYSTEM_ENV_CORRUPTION | 0.3 | 0.5 | 0.3 | 0.5 | 0.6 | 0.6 | 0.6 | 1 | 0.6 | 0.3 | 0.4 | 0.1 | 0.5 | 0.6 |
| USER_ENV_CORRUPTION | 0.3 | 0.5 | 0.5 | 0.3 | 0.6 | 0.6 | 0.6 | 0.6 | 1 | 0.3 | 0.4 | 0.1 | 0.5 | 0.6 |
| ASSET_DISTRESS | 0.3 | 0.3 | 0.3 | 0.6 | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 1 | 0.4 | 0.4 | 0.3 | 0.6 |
| SUSPICIOUS_USAGE | 0.3 | 0.3 | 0.5 | 0.3 | 0.5 | 0.6 | 0.5 | 0.6 | 0.5 | 0.3 | 1 | 0.1 | 0.3 | 0.6 |
| CONNECTION_VIOLATION | 0.3 | 0.1 | 0.1 | 0.3 | 0.8 | 0.3 | 0.3 | 0.3 | 0.3 | 0.5 | 0.4 | 1 | 0.3 | 0.6 |
| BINARY_SUBVERSION | 0.3 | 0.3 | 0.3 | 0.3 | 0.3 | 0.6 | 0.6 | 0.6 | 0.5 | 0.3 | 0.4 | 0.1 | 1 | 0.6 |
| ACTION_LOGGED | 0.3 | 0.3 | 0.3 | 0.3 | 0.6 | 0.5 | 0.3 | 0.3 | 0.3 | 0.3 | 0.4 | 0.3 | 0.3 | 1 |

**Figure 5**

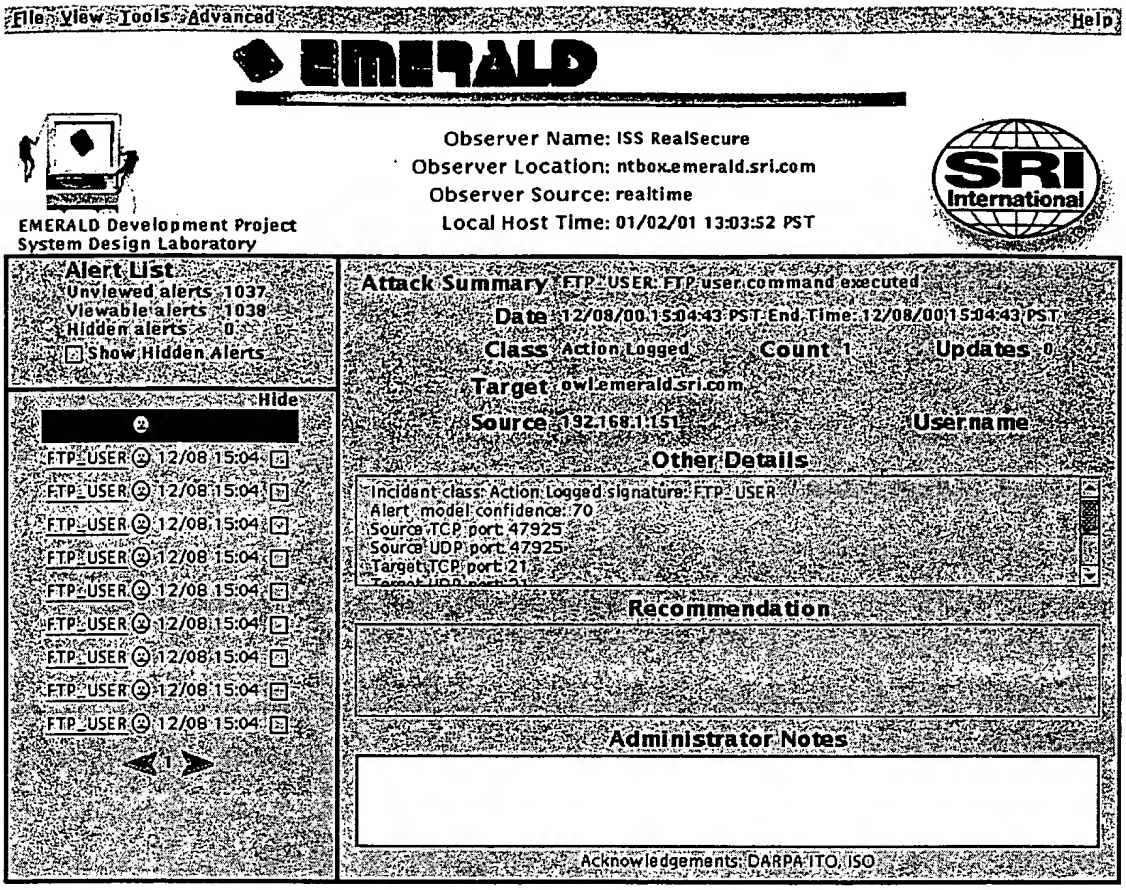
File View Tools Advanced Help
EMERALD
Observer Name: ISS RealSecure
Observer Location: ntbox.emerald.sri.com
Observer Source: realtime
Local Host Time: 01/02/01 13:03:52 PST
EMERALD Development Project
System Design Laboratory
SRI International
Alert List
Unviewed alerts 1037
Viewable alerts 1038
Hidden alerts 0
Show Hidden Alerts
Hide
FTP_USER 12/08 15:04
Attack Summary FTP_USER: FTP user command executed
Date 12/08/00 15:04:43 PST End Time: 12/08/00 15:04:43 PST
Class Action Logged Count 1 Updates 0
Target owl.emerald.sri.com
Source 192.168.1.151 User name
Other Details
Incident class: Action Logged signature: FTP_USER
Alert model confidence: 70
Source TCP port 47925
Source UDP port 47925
Target TCP port 21
Recommendation
Administrator Notes
Acknowledgements: DARPA ITO, ISO

Figure 6

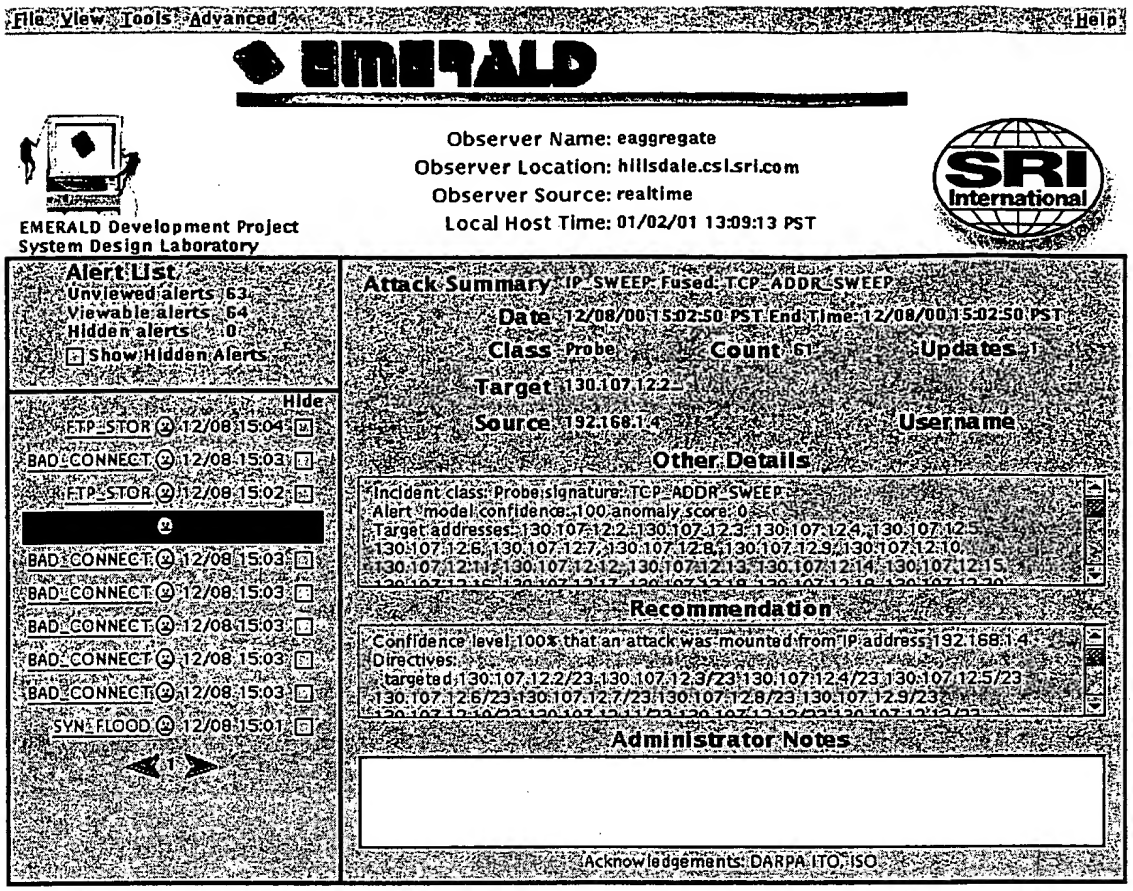
File View Tools Advanced Help
EMERALD
EMERALD Development Project
System Design Laboratory
Observer Name: eaggregate
Observer Location: hillsdale.csl.sri.com
Observer Source: realtime
Local Host Time: 01/02/01 13:09:13 PST
SRI International
Alert List
Unviewed alerts 63
Viewable alerts 64
Hidden alerts 0
Show Hidden Alerts
Hide
FTP_STOR 12/08 15:04
BAD_CONNECT 12/08 15:03
FTP_STOR 12/08 15:02
BAD_CONNECT 12/08 15:03
BAD_CONNECT 12/08 15:03
BAD_CONNECT 12/08 15:03
BAD_CONNECT 12/08 15:03
BAD_CONNECT 12/08 15:03
SYN_FLOOD 12/08 15:01
Attack Summary IP_SWEEP Fused_TCP_ADDR_SWEEP
Date 12/08/00 15:02:50 PST End Time: 12/08/00 15:02:50 PST
Class Probe Count 61 Updates 1
Target 130.107.12.2
Source 192.168.1.4
Username
Other Details
Incident class: Probe signature: TCP_ADDR_SWEEP
Alert model confidence: 100 anomaly score: 0
Target addresses: 130.107.12.2, 130.107.12.3, 130.107.12.4, 130.107.12.5, 130.107.12.6, 130.107.12.7, 130.107.12.8, 130.107.12.9, 130.107.12.10, 130.107.12.11, 130.107.12.12, 130.107.12.13, 130.107.12.14, 130.107.12.15,
Recommendation
Confidence level 100% that an attack was mounted from IP address 192.168.1.4
Directives:
targeted 130.107.12.2/23 130.107.12.3/23 130.107.12.4/23 130.107.12.5/23 130.107.12.6/23 130.107.12.7/23 130.107.12.8/23 130.107.12.9/23
Administrator Notes
Acknowledgements: DARPA ITO, ISO

Figure 7

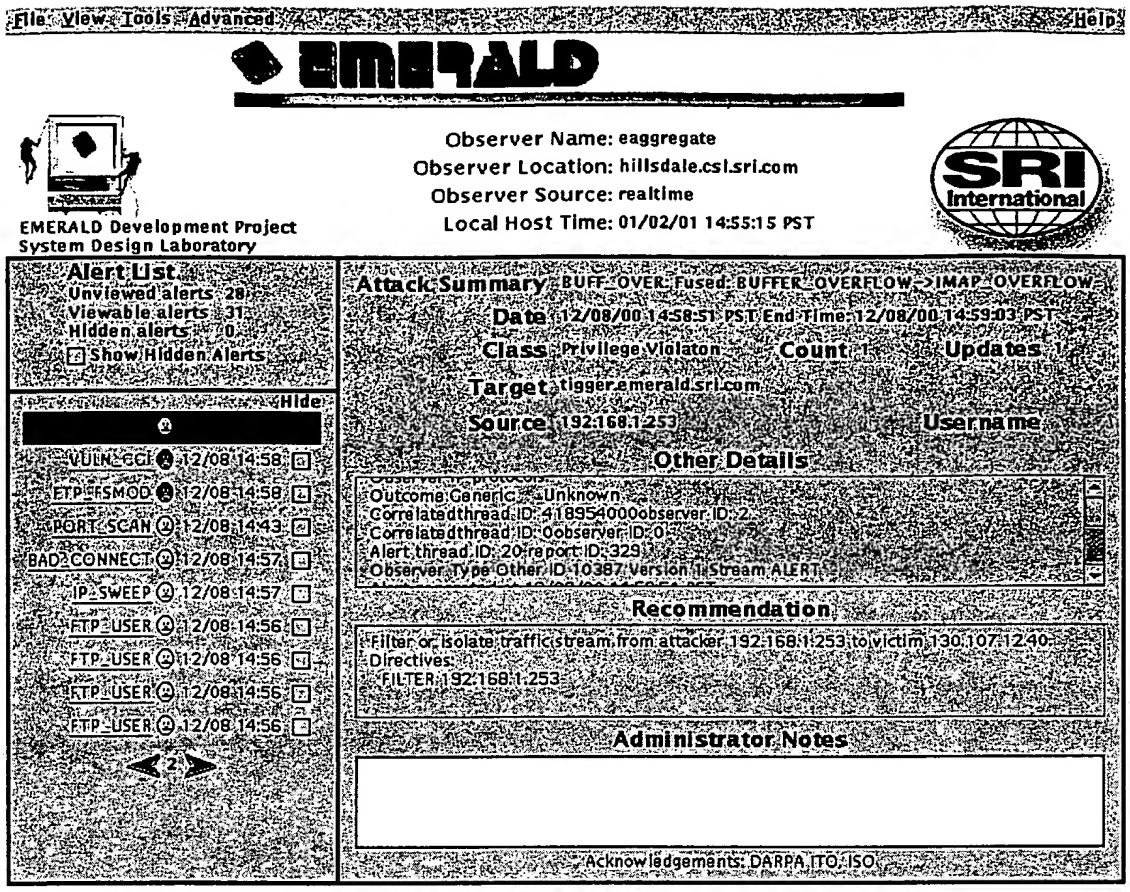
File View Tools Advanced Help
EMERALD
EMERALD Development Project
System Design Laboratory
Observer Name: eaggregate
Observer Location: hillsdale.csl.sri.com
Observer Source: realtime
Local Host Time: 01/02/01 14:55:15 PST
SRI International
Alert List
Unviewed alerts: 28
Viewable alerts: 31
Hidden alerts: 0
Show Hidden Alerts
Hide
VULN_CGI 12/08 14:58
FTP_FSMOD 12/08 14:58
PORT_SCAN 12/08 14:43
BAD2CONNECT 12/08 14:57
IP_SWEEP 12/08 14:57
FTP_USER 12/08 14:56
FTP_USER 12/08 14:56
FTP_USER 12/08 14:56
FTP_USER 12/08 14:56
2
Attack Summary: BUFF_OVER_Fused: BUFFER_OVERFLOW->IMAP_OVERFLOW
Date: 12/08/00 14:58:51 PST End Time: 12/08/00 14:59:03 PST
Class: Privilege Violaton Count: 1 Updates
Target: tigger.emerald.sri.com
Source: 192.168.1.253 Username
Other Details
Outcome: Generic Unknown
Correlatedthread ID: 4189540000bserver ID: 2
Correlatedthread ID: 0observer ID: 0
Alert thread ID: 20 report ID: 329
Observer Type: Other ID: 10387 Version: 1 Stream: ALERT
Recommendation
Filter or isolate traffic stream from attacker 192.168.1.253 to victim 130.107.12.40
Directives:
FILTER 192.168.1.253
Administrator Notes
Acknowledgements: DARPA ITO ISO

Figure 8

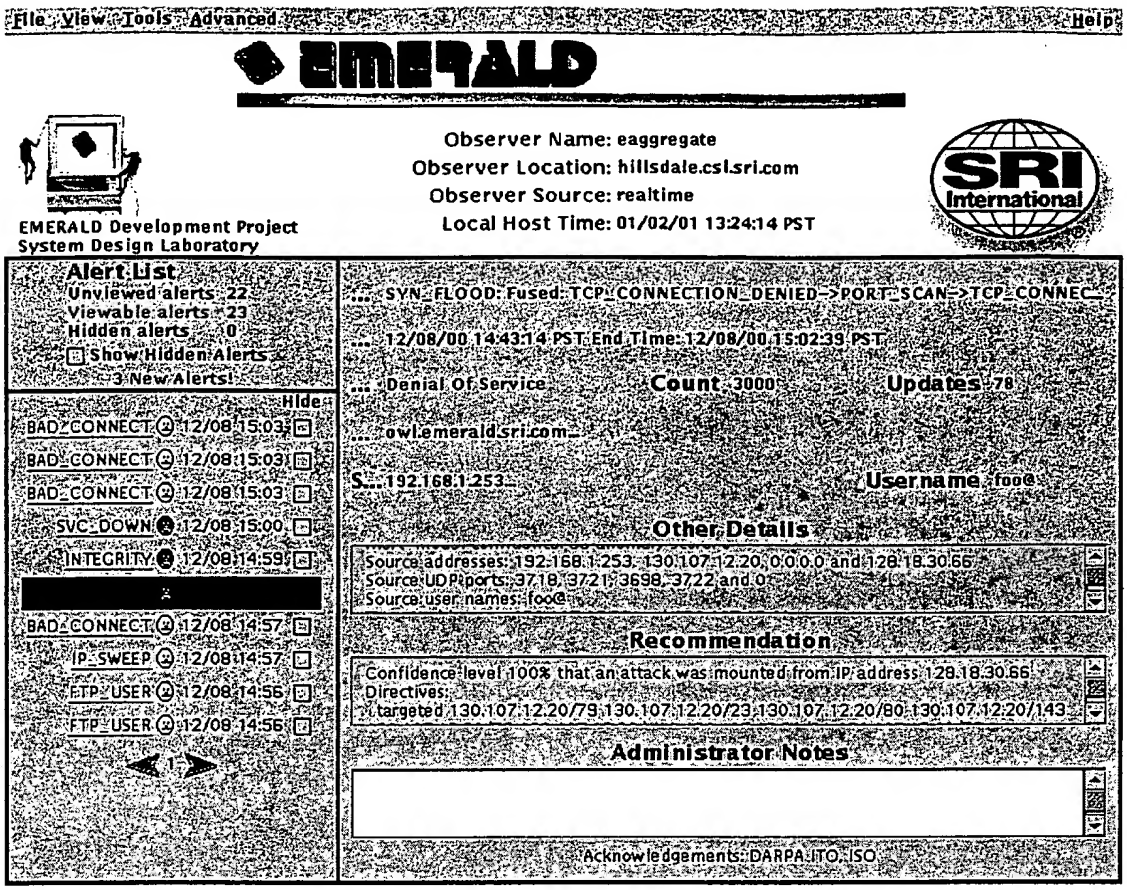
File View Tools Advanced Help
EMERALD
Observer Name: eaggregate
Observer Location: hillsdale.csl.sri.com
Observer Source: realtime
Local Host Time: 01/02/01 13:24:14 PST
EMERALD Development Project
System Design Laboratory
SRI International
Alert List
Unviewed alerts: 22
Viewable alerts: 23
Hidden alerts: 0
Show Hidden Alerts
3 New Alerts!
Hide
BAD_CONNECT 12/08 15:03
BAD_CONNECT 12/08 15:03
BAD_CONNECT 12/08 15:03
SVC_DOWN 12/08 15:00
INTEGRITY 12/08 14:59
BAD_CONNECT 12/08 14:57
IP_SWEEP 12/08 14:57
FTP_USER 12/08 14:56
FTP_USER 12/08 14:56
SYN_FLOOD: Fused: TCP_CONNECTION_DENIED->PORT_SCAN->TCP_CONNEC
12/08/00 14:43:14 PST End Time: 12/08/00 15:02:39 PST
Denial Of Service
Count: 3000
Updates: 78
owl.emerald.sri.com
S: 192.168.1.253
Username: foo@
Other Details
Source addresses: 192.168.1.253, 130.107.12.20, 0.0.0.0 and 128.18.30.66
Source UDP ports: 3718, 3721, 3698, 3722 and 0
Source user names: foo@
Recommendation
Confidence level 100% that an attack was mounted from IP address 128.18.30.66
Directives:
targeted 130.107.12.20/79,130.107.12.20/23,130.107.12.20/80,130.107.12.20/143
Administrator Notes
Acknowledgements: DARPA, ITO, ISO

Figure 9